UNITED STATES DISTRICT COURT
NORTHERN DISTRICT OF GEORGIA
ATLANTA DIVISION

JEREMY MERRITT, GARY GILCHRIST, and TRAVIS RUSSELL, Individually and on Behalf of all Others Similarly Situated,	)	
PLAINTIFFS,	)	
v.	)	CASE NO. _____
HOME DEPOT U.S.A., INC.,	)	
DEFENDANT.	)	

CLASS ACTION COMPLAINT

Plaintiffs Jeremy Merritt, Gary Gilchrist and Travis Russell ("Plaintiffs"), individually and on behalf of the Classes defined below of similarly situated persons, allege the following against Home Depot U.S.A., Inc. ("Home Depot" or "Defendant") based upon personal knowledge with respect to themselves and on information and belief derived from, among other things, investigation of counsel and review of public documents as to all other matters:

NATURE OF THE CASE

1. Plaintiffs bring this consumer class action against Home Depot for its failure to secure and safeguard its customers' credit and debit card numbers, three-digit security codes and other payment card data ("PCD"), personally identifiable information such as the cardholder's names, mailing addresses, e-mail addresses and other personal information ("PII") (collectively "Personal Information"), and for failing to provide timely and adequate notice to Plaintiffs and other Class members that their Personal Information had been stolen and precisely what types of information were stolen.

2. Home Depot permitted unauthorized access of its customers' Personal Information from April of 2014 to at least September 2, 2014 in its U.S. and Canadian stores. As a result of Home Depot's own acts and omissions, Home Depot's point-of-sale system exposed Defendant Home Depot's customers' Personal Information to criminals. The Personal Information of millions of Home Depot customers was accessed without their knowledge or authorization, including debit and credit card account information (the "Data Breach").

3. On September 2, 2014, security blogger Brian Krebs first reported that "[m]ultiple banks say they are seeing evidence that Home Depot stores may be the

source of a massive new batch of stolen credit and debit cards that went on sale this morning in the cybercrime underground."[1]

4. That same day, after the facts of the data breach were made public, Home Depot issued a statement disclosing only that there "might" be a "possible payment data breach." This statement was not one designed to notify affected customers directly. Instead, Home Depot posted the statement on its corporate website and not on the front page of the Home Depot shopping site regularly accessed by customers.

5. On September 7, 2014, Brian Krebs reported that Home Depot's store registers had been infected with a new variant of "BlackPOS," the malicious software (or malware) used to perpetrate the widely-reported Target Corporation data breach.[2] Krebs further reported that "[c]lues buried within this newer version of BlackPOS support the theory put forth by multiple banks that the Home Depot breach may involve compromised store transactions going back at least several months."[3]

---

[1] <http://krebsonsecurity.com/2014/09/banks-credit-card-breach-at-home-depot/> (last visited Sept. 18, 2014).

[2] <http://krebsonsecurity.com/2014/09/home-depot-hit-by-same-malware-as-target/> (last visited Sept. 18, 2014).

[3] *Id.*

6. On September 8, 2014, six days after the breach was first reported, Home Depot finally issued a press release confirming the massive breach of its customers' Personal Information.[4] Since that time, Home Depot has yet to confirm or fully disclose what types of Personal Information were stolen.

7. Experts believe that Home Depot's data breach could be significantly larger than the massive data breach experienced by Target Corporation. Indeed, more than 60 million credit card numbers may have already been stolen from Home Depot's payment system. "Comparatively, hackers stole data for over 40 million cards from Target's system following a three-week attack during the busy Black Friday shopping season. However, the breach at Home Depot went undetected for a much longer period of time . . . all customers that have shopped in a retail store in the U.S. or Canada (more than 2,250 locations, 400 more than affected Target stores) and paid with a debit or credit card."[5]

8. Home Depot's security protocols were so deficient that the Data Breach continued for nearly five months while Home Depot failed to even detect it. Home Depot disregarded Plaintiffs' and Class members' rights by intentionally,

[4] <https://corporate.homedepot.com/MediaCenter/Documents/Press%20Release.pdf> (last visited Sept. 18, 2014).

[5] <http://news.yahoo.com/home-depot-massive-credit-card-data-breach-may-105054766.html> (last visited Sept. 18, 2014).

willfully, recklessly, or negligently failing to take adequate and reasonable measures to ensure its data systems were protected, failing to take available steps to prevent and stop the breach from ever happening, and failing to disclose to its customers the material facts that it did not have adequate computer systems and security practices to safeguard customers' Personal Information.

9. Plaintiffs, on behalf of themselves and others similarly situated, assert claims for negligence, breach of implied contract, violations of the Florida Deceptive and Unfair Trade Practices Act, Fla. Stat. Ann. §§ 501.201, *et seq*., and seek injunctive relief, declaratory relief, monetary damages, statutory damages, and all other relief as authorized in equity or by law.

JURISDICTION AND VENUE

10. This Court has jurisdiction over this action under the Class Action Fairness Act, 28 U.S.C. § 1332(d)(2). The amount in controversy exceeds $5 million exclusive of interest and costs. At least one Plaintiff and Defendant are citizens of different states. There are more than 100 putative class members.

11. This Court has personal jurisdiction over Home Depot because the company maintains its principal place of business in Georgia, regularly conducts business in Georgia, and has sufficient minimum contacts in Georgia. Home Depot intentionally avails itself of this jurisdiction by marketing and selling products

from Georgia to millions of consumers nationwide. Venue is proper in this Court pursuant to 28 U.S.C. § 1391(a) because Home Depot's principal place of business is in this district and a substantial part of the events, acts, and omissions giving rise to Plaintiffs' claims occurred in this District.

PARTIES

12. Plaintiff Jeremy Merritt, a resident of Carmel, Indiana, used his American Express credit card to purchase goods at a Home Depot store during the period of the Data Breach. Plaintiff Merritt's personal information associated with his credit card was compromised as a result of the Home Depot data breach. Plaintiff Merritt was harmed by having his financial and personal information compromised. He incurred three unauthorized charges totaling approximately $66 on June 26, 2014. When American Express notified Plaintiff Merritt of the unauthorized charges and subsequently canceled his card, Plaintiff Merritt was traveling and did not have access to alternative credit or debit card funds. As a result, Plaintiff Merritt had to travel with very limited access to funds which included only the cash he had on his person. Plaintiff Merritt also lost access to his account funds and spent time resetting automatic payment instructions for his accounts as a result of the Home Depot Data Breach.

13. Plaintiff Gary Gilchrist, a resident of Palm Harbor, Florida, used his USAA MasterCard credit card to purchase goods at a Home Depot store during the period of the Data Breach. Plaintiff Gilchrist's personal information associated with his credit card was compromised as a result of the Home Depot data breach. Plaintiff Gilchrist was harmed by having his financial and personal information compromised. He incurred an unauthorized charge of approximately $125.00 on June 20, 2014.

14. Plaintiff Travis Russell, a resident of West Fargo, North Dakota, used his USAA MasterCard credit card to make multiple purchases of goods at a Home Depot store during the period of the Data Breach. Plaintiff Russell's personal information associated with his credit card was compromised as a result of the Home Depot data breach. Plaintiff Russell was harmed by having his financial and personal information compromised and faces the imminent and certainly impending threat of future additional harm from the increased threat of identity theft and fraud due to his financial and personal information being sold on the Internet black market and/or misused by criminals. Plaintiff Russell also spent time resetting automatic payment instructions for his accounts as a result of the Home Depot Data Breach.

15. Defendant Home Depot is a Delaware corporation with its headquarters at 2455 Paces Ferry Road, Atlanta, Georgia, 30339. Home Depot operates retail stores throughout the United States. Home Depot can be served with served with process through its registered agent at CSC of Cobb County, Inc. at 192 Anderson Street S.E., Suite 125 Marietta, Georgia 30060.

FACTUAL BACKGROUND

Home Depot's Information Collection

16. Home Depot operates approximately 1,977 retail stores in the United States and another 180 in Canada. Home Depot is the world's largest home improvement retailer and fourth largest retailer in the United States. In 2013, Home Depot generated $78.8 billion in sales and $5.4 billion in profit.

17. When consumers make purchases at Home Depot retail stores using credit or debit cards, Home Depot collects PCD related to those cards including the card holder name, the account number, expiration date, card verification value, and PIN data for debit cards. Home Depot stores the PCD in its point-of-sale system and transmits this information to a third party for completion of the payment. Home Depot also collects and stores PII, including but not limited to customer names, mailing addresses, phone numbers, and email addresses.

18. Home Depot uses consumers' Personal Information in ways that greatly exceed the expectations of customers. Through its Privacy Policy, which is available on its website, Home Depot identifies the categories of Personal Information it collects:

> **Information We Collect**
>
> **Contact information**
> We may collect the names and user names of our customers and other visitors. Additionally, we may collect your purchase history, billing and shipping addresses, phone numbers, email addresses, and other digital contact information. We may also collect information that you provide us about others.
>
> **Payment information**
> When you make a purchase we collect your payment information, including information from your credit or debit card, check, PayPal account or gift card. If you apply for a The Home Depot credit card or a home improvement loan, we might collect information related to your application.
>
> **Returns information**
> When you return a product to our stores or request a refund or exchange, we may collect information from you and ask you to provide your government issued ID. We use the information we collect from you and capture off of your government issued ID to help prevent fraud. To learn more about our Returns Policy, click here.
>
> **Demographic information**
> We may collect information about products or services you like, reviews you submit, or where you shop. We might also collect information like your age or gender.
>
> **Location information**
> If you use our mobile websites or applications, we may collect location data obtained from your mobile device's GPS. If you use our websites, we may collect location data obtained from your IP address.

> We use this location data to find our nearest store to you, product availability at our stores near you and driving directions to our stores.
>
> **Other information**
> If you use our websites, we may collect information about the browser you are using. We might track the pages you visit, look at what website you came from, or what website you visit when you leave us. We collect this information using the tracking tools described here. To control those tools, please read the Your Privacy Preferences section.[6]

19. Home Depot collects Personal Information not only from point-of-sale purchases, but also "passively" from "tracking tools like browser cookies, flash cookies, and web beacons," and from "other sources" like "third party business partners."[7]

20. The information is used for any number of purposes including "[e]ntering you into a sweepstakes or sending you prizes you might have won;" for "security purposes . . . to protect [Home Depot and its] customers;" and "for [Home Depot's] marketing." Personal information collected by Home Depot is also shared with "third parties who perform services on [Home Depot's] behalf;" "to offer financial products, such as The Home Depot credit card and home improvement loans;" for "Data Sharing for Catalog Mailings" and even to "protect [Home Depot] . . .if [Home Depot] suspect[s] fraud."[8]

---

[6] <http://www.homedepot.com/c/Privacy_Security> (last visited Sept. 18, 2014).

[7] *Id.*

[8] *Id.*

21. Any associate of Home Depot can access complete sales data on any credit, debit, or check transaction via a browser-based terminal or point-of-sale device. Home Depot compiles and maintains files concerning consumers' financial and credit histories. Home Depot regularly engages, in part, in the practice of assembling and/or evaluating consumer credit information or other information. Home Depot supplies that information to third-parties, including banks. Defendant Home Depot's collection, maintenance and dissemination of its customers' data, relates, in part, to the customers' credit worthiness, credit standing, credit capacity, character, general reputation, personal characteristics, or mode of living, and is, from time to time, used or expected to be used or collected for the purpose of serving as a factor in establishing eligibility for credit, including for Home Depot's credit card or home improvement loans.

22. Thus, Home Depot stores massive amounts of Personal Information on its servers and utilizes this information, not to protect the Personal Information of its customers, but to maximize its profits through third-party affiliates, predictive marketing and other marketing techniques.

23. Consumers place value in data privacy and security, and they consider it when making purchasing decisions. Plaintiffs would not have made purchases at Home Depot, or would not have paid as much for the goods they purchased, had

they known that Home Depot does not take all necessary precautions to secure their personal and financial data.

24. Furthermore, when consumers purchase goods at a national retailer, such as Home Depot, they assume that its data security practices and policies are state-of-the-art and that the retailer will use part of the purchase price that consumers pay for such state-of-the-art practices. Consumers thus enter into an implied contract with Home Depot that Home Depot will adequately secure and protect their Personal Information, and will use part of the purchase price of the goods to pay for adequate data security measures. In fact, rather than use those moneys to implement adequate data security policies and procedures, Home Depot failed to provide reasonable security measures, thereby breaching its implied contract with Plaintiffs.

Home Depot Failed to Comply With Industry Standards

25. Home Depot accepts customer payment for goods or services made by credit and debit cards issued by members of the Payment Card Industry, such as Visa, MasterCard, Discover, and American Express.

26. Unlike PII data, PCD (or payment card data) is heavily regulated. The Payment Card Industry Security Standards Council formed a body of security standards known as the PCI Data Security Standards ("PCI DSS") which consist of

significant requirements including multiple sub-requirements which contain numerous directives against which businesses may measure their own payment card security policies, procedures and guidelines.

27. The PCI DSS was developed to encourage and enhance cardholder data security and facilitate the broad adoption of consistent data security measures globally. PCI DSS provides a baseline of technical and operational requirements designed to protect cardholder data. PCI DSS applies to all entities involved in payment card processing—including merchants, processors, acquirers, issuers, and service providers, as well as all other entities that store, process or transmit cardholder data and/or sensitive authentication data.[9]

28. PCI DSS requires merchants to: build and maintain a secure network and system; protect cardholder data; maintain a vulnerability and management program; implement strong access control measures; regularly monitor and test networks; and maintain an information security policy.[10]

29. Home Depot is contractually-obligated to fully comply with all of the PCI DSS requirements and individual PCI members' requirements as a condition of being permitted to process transactions through the PCI members' networks.

---

[9] <https://www.pcisecuritystandards.org/documents/PCI_DSS_v3.pdf> (last visited Sept. 18, 2014).

[10] *Id*.

30. At all times relevant to this action, Home Depot held itself out as comporting with PCI DSS and was, therefore, authorized by PCI members to accept credit and debit cards for the payment of personal goods and services.

31. The PCI DSS is an industry standard for large retail institutions that accept credit card and debit card transactions. The standard consists of 12 general requirements:

a. Install and maintain a firewall configuration to protect cardholder data;

b. Do not use vendor-supplied defaults for system passwords and other security parameters;

c. Protect stored cardholder data;

d. Encrypt transmission of cardholder data and sensitive information across public networks;

e. Protect all systems against malware and regularly update anti-virus software or programs;

f. Develop and maintain secure systems and applications;

g. Restrict access to cardholder data by business need-to-know;

h. Identify and authenticate access to system components;

i. Restrict physical access to cardholder data;

j. Track and monitor all access to network resources and cardholder data;

k. Regularly test security systems and processes; and

l. Maintain a policy that addresses information security for all personnel.[11]

32. Additionally, financial institutions and credit card processing companies have issued rules and standards governing the basic measures that merchants such as Home Depot must take to ensure that valuable transactional data is secure and protected. The debit and credit card companies issue regulations ("Card Operating Regulations") that bind Home Depot as a condition of its contract with its acquiring bank. The Card Operating Regulations prohibit Home Depot and other merchants from disclosing any card holder account numbers, personal information, magnetic stripe information or transaction information to third parties (other than the merchant's agent, the acquiring bank, or the acquiring bank's agents). The Card Operating Regulations further require Home Depot to maintain the security and confidentiality of debit and credit cardholder information and magnetic stripe information and protect it from unauthorized disclosure.

[11] *Id.*

33. Despite Home Depot's awareness of its data protection obligations, Home Depot's treatment of the financial account and personally identifying information entrusted to it by its customers fell far short of satisfying Home Depot's legal duties and obligations. Home Depot failed to ensure that access to its data systems was reasonably safeguarded. Home Depot failed to acknowledge and act upon numerous warning signs and properly utilize its own security systems that were put in place to detect and deter this exact type of attack.

34. Home Depot did not comply with the PCI DSS or Card Operating Regulations. As a result of Home Depot's inadequate data security, cyber-criminals now possess the personal and financial information of Plaintiffs and the Class. While credit card companies offer protection against unauthorized charges, the process is long, costly, and frustrating. Physical cards must be replaced, credit card information must be updated on all automatic payment accounts, and victims must add themselves to credit fraud watch lists, which substantially impair victims' ability to obtain additional credit.

The Home Depot Data Breach

35. On September 2, 2014, Home Depot's banking partners and law enforcement officials notified the retailer of a potential data breach involving the theft of its customers' credit card and debit card data.

36. That same day, multiple banks began reporting evidence that Home Depot stores were the likely source of a massive batch of stolen card data that went on sale that morning at rescator.cc, the same underground cybercrime shop that sold millions of cards stolen in the 2013 attack on Target.[12]

37. Specifically, according to security blogger Brian Krebs of Krebs on Security (the "Krebs Report"), the cybercrime store rescator.cc (the "Rescator website") listed consumer credit cards for sale that, with the unique ZIP code and other card data, at least four banks had traced back to previous transactions at Home Depot.

38. The Krebs Report explained that "experienced crooks prefer to purchase cards that were stolen from stores near them, because they know that using the cards for fraudulent purchases in the same geographic area as the legitimate cardholder is less likely to trigger alerts about suspicious transactions—alerts that could render the stolen card data worthless for the thieves."[13] The Krebs Report indicated a "staggering 99.4 percent overlap" between the unique ZIP codes represented on the Rescator website and those of Home Depot stores, strongly

[12] <http://krebsonsecurity.com/2014/09/home-depot-hit-by-same-malware-as-target/> (last visited Sept. 18, 2014).

[13] <http://krebsonsecurity.com/2014/09/data-nearly-all-u-s-home-depot-stores-hit/> (last visited Sept. 18, 2013).

suggesting that the source of the breached credit card data was from Home Depot.[14]

39. The ZIP code information the Krebs Report pulled from the Rescator website appears to represent the vast majority, if not all, of Home Depot's approximately 2,000 domestic retail locations. The Krebs Report further indicated that, based on conversations with affected banks, this data breach "probably started in late April or early May" and may be ongoing, potentially dwarfing the 40 million debit and credit cards affected by the recent Target data breach (which had 1,800 stores affected during a period of approximately 3 weeks).

40. After this news broke, on September 3, 2014, Home Depot released an ambiguous and uninformative statement buried on its corporate site (not the Internet site visited by consumers) that failed to confirm the Data Breach:

> We're looking into some unusual activity that might indicate a possible payment data breach and we're working with our banking partners and law enforcement to investigate. We know that this news may be concerning and we apologize for the worry this can create. If we confirm a breach has occurred, we will make sure our customers are notified immediately.[15]

[14] *Id.*

[15] <http://patch.com/massachusetts/concord/home-depot-investigating-possible-data-breach-0#.VBmySvldUjY> (last visited Sept. 18, 2014).

41. On September 8, 2014, Home Depot confirmed that its systems had been breached and conceded that compromised information may include "[p]ayment card information such as name, credit card number, expiration date, cardholder verification value and service code for purchases made at Home Depot stores in 2014, from April on."[16]

42. Home Depot has not indicated whether social security numbers, PIN numbers and dates of birth were compromised, nor has it disclosed whether the wide range of other PII that it collects, including names, addresses, telephone numbers, mobile telephone numbers, driver's license numbers, bank account numbers, email addresses, computer IP addresses, and location information, were disclosed in the breach.[17]

43. Without such detailed disclosure, Plaintiffs and Class members are unable to take the necessary precautions to prevent imminent harm, such as continued misuse of their personal information.

44. "The stolen card data being offered for sale on [the Rescator website] includes both the information needed to fabricate counterfeit cards as well *as the legitimate cardholder's full name* and the city, state and ZIP of the Home Depot

[16]<https://corporate.homedepot.com/MediaCenter/Documents/Required%20Regulatory%20Notice.PDF> (last visited Sept. 18, 2014).

[17] *Id*.

store from which the card was stolen."[18] Information pertaining to the cardholder's location allows hackers to obtain a cardholder's Social Security number and date of birth, further increasing the risk of identity theft (above and beyond fraudulent credit and/or debit card transactions) for affected Home Depot customers.

45. Thieves already are using the Personal Information stolen from Home Depot to commit actual fraud. Some thieves are using the Personal Information to change a cardholder's PIN numbers on stolen debit cards and to make ATM withdrawals from Home Depot customer's accounts. On September 8, 2014, a bank located on the West Coast reported that it "lost more than $300,000 in two hours today to PIN fraud on multiple debit cards that had all been used recently at Home Depot."[19] On that same day, the Krebs Report advised that multiple financial institutions had reported "a steep increase over the past few days in fraudulent ATM withdrawals on customer accounts."[20]

46. The Data Breach was caused and enabled by Home Depot's violation of its obligations to abide by best practices and industry standards in protecting its customers' Personal Information.

---

[18] <http://krebsonsecurity.com/2014/09/in-wake-of-confirmed-breach-at-home-depotbanks-see-spike-in-pin-debit-card-fraud/> (last visited Sept. 18, 2014).

[19] *Id.*

[20] *Id.*

47. The software used in the attack was a variant of "BlackPOS," a malware strain designed to siphon data from cards when they are swiped at infected point-of-sale systems.[21] Hackers had previously utilized BlackPOS in other recent cyber-attacks, including the 2013 breach at Target. While many retailers, banks and card companies have responded to these recent breaches by adopting technology and security practices that help makes transactions and stored data more secure, Home Depot did not do so.

48. Moreover, in July 2014, the Homeland Security Department and the Secret Service issued a report warning retailers to check their in-store cash register systems for a set of malware that could evade detection of antivirus products.[22] On information and belief, Home Depot could have taken immediate action to ensure that its consumers' Personal Information would not continue to be available to hackers and identity thieves, but Home Depot chose not to take such action.

49. According to *Bloomberg*, managers within the company stated that Home Depot was using out-of-date anti-virus software on its point-of-sale devices. They noted that while Home Depot had purchased software designed to encrypt

[21] <http://krebsonsecurity.com/2014/09/home-depot-hit-by-same-malware-as-target/> (last visited Sept. 18, 2014).

[22] <http://www.nytimes.com/2014/09/03/technology/home-depot-data-breach.html?_r=0> (last visited Sept. 18, 2014).

credit card data when it was being sent from POS devices to central servers, Home Depot had yet to implement the software. The sources also stated that Home Depot's technology executives were underfunding the company's information security program, leading to higher-than-average levels of security staff turnover.[23]

50. On September 19, 2014, an article in the *New York Times* confirmed that former employees were raising alarms in Home Depot's cyber-security as far back as 2008.[24] Indeed, the article suggested that "Home Depot relied on outdated software to protect its network and scanned systems that handled customer information irregularly, those [former employees] said. Some members of its security team left as managers dismissed their concerns. Others wondered how Home Depot met industry standards for protecting customer data. One went so far as to warn friends to use cash, rather than credit cards, at the company's stores."[25]

51. According to the *New York Times* article, "Home Depot's security group in recent years said managers failed to take such threats as seriously as they should have. They said managers relied on outdated Symantec antivirus software from 2007 and did not continuously monitor the network for unusual behavior,

[23] <http://www.businessweek.com/articles/2014-09-12/home-depot-didnt-encrypt-credit-card-data-former-workers-say> (last visited Sept. 18, 2014).

[24] <http://www.nytimes.com/2014/09/20/business/ex-employees-say-home-depot-left-data-vulnerable.html> (last visited Sept. 22, 2014).

[25] *Id*.

such as a strange server talking to its checkout registers. Also, the company performed vulnerability scans irregularly on the dozen or so computer systems inside its stores and often scanned only a small number of stores. Credit card industry security rules require large retailers like Home Depot to conduct such scans at least once a quarter, using technologies approved by the Payment Card Industry Security Standards Council, which develops technical requirements for its members' data security programs. The P.C.I. Council requires that approved, third-party quality security assessors perform routine tests to ensure that merchants are compliant." As noted in the article "scanning is the easiest part of compliance."[26]

52. Home Depot clearly failed to implement and maintain reasonable security procedures and practices appropriate to the nature and scope of the Personal Information compromised in the Data Breach which directly resulted in the theft and resale of its customers' Personal Information.

Stolen Personal Information Is Valuable to Hackers and Thieves

53. Personal and financial information is a valuable commodity. A "cyber black-market" exists in which criminals openly post stolen credit card numbers, Social Security numbers, and other personal information on a number of Internet websites. Indeed, the personal and financial information that Home Depot failed to

[26] *Id.*

adequately protect, including Plaintiffs' identifying information, is as good as gold to identity thieves because identity thieves can use victims' personal data to open new financial accounts and incur charges in another person's name, take out loans in another person's name, incur charges on existing accounts, or clone ATM, debit, or credit cards.

54. Plaintiffs' and Class members' personal and financial information stolen from Home Depot has flooded the underground black market with card numbers selling between $9 and $50 per card, with business cards, platinum levels and American Express Centurion Cards commanding higher prices.[27]

55. The online black markets also provide purchasing thieves with the zip code and location of the Home Depot store where the information was stolen. This allows thieves to make same-state purchases, thus avoiding any blocks from banks who suspect fraud. As noted by Krebs, "[t]he card data stolen from Home Depot customers and now for sale . . . includes both the information needed to fabricate counterfeit cards as well as the legitimate cardholder's full name and the city, state and ZIP of the Home Depot store from which the card was stolen (presumably by malware installed on some part of the retailer's network, and probably on each point-of-sale device). *This is especially helpful for fraudsters since most Home*

[27] <http://www.bankinfosecurity.com/analysis-home-depot-breach-details-a-7323> (last visited Sept. 18, 2014).

Depot transactions are likely to occur in the same or nearby ZIP code as the cardholder."[28]

56. The ramifications of Home Depot's failure to keep Class members' data are severe. Identity thieves can use personal information such as that of Class members, which Home Depot failed to keep secure, to perpetrate a variety of crimes that harm victims. For instance, identity thieves may commit various types of government fraud such as: immigration fraud; obtaining a driver's license or identification card in the victim's name but with another's picture; using the victim's information to obtain government benefits; or filing a fraudulent tax return using the victim's information to obtain a fraudulent refund. Some of this activity may not come to light for years.

57. In addition, identity thieves may get medical services using consumers' compromised personal information or commit any number of other frauds, such as obtaining a job, procuring housing, or even giving false information to police during an arrest.

58. It is incorrect to assume that reimbursing a consumer for fraud makes that individual whole again. On the contrary, after conducting a study, the Department of Justice's Bureau of Justice Statistics ("BJS") found that "among

[28] <http://krebsonsecurity.com/2014/09/in-wake-of-confirmed-breach-at-home-depot-banks-see-spike-in-pin-debit-card-fraud/> (last visited Sept. 18, 2014).

victims who had personal information used for fraudulent purposes, 29% spent a month or more resolving problems."[29]

59. Additionally, there is commonly lag time between when harm occurs versus when it is discovered, and also between when PII or PCD is stolen and when it is used. According to the U.S. Government Accountability Office, which conducted a study regarding data breaches:

> [L]aw enforcement officials told us that in some cases, stolen data may be held for up to a year or more before being used to commit identity theft. Further, once stolen data have been sold or posted on the Web, fraudulent use of that information may continue for years. As a result, studies that attempt to measure the harm resulting from data breaches cannot necessarily rule out all future harm.[30]

60. There is a very strong probability that entire batches of stolen card data have yet to be dumped on the black market, meaning Home Depot customers could be at risk of fraud and identity theft for extended periods of time, perhaps even longer than the one year of credit monitoring Home Depot has offered its customers.

61. Plaintiffs and the Class have or will suffer actual injury as a direct result of the Data Breach. This not only includes experiencing fraudulent charges

[29] <http://www.bjs.gov/content/pub/pdf/vit12.pdf> (last visited Sept. 18, 2014).

[30] <http://www.gao.gov/new.items/d07737.pdf> (last visited Sept. 18, 2014).

on their credit and debit accounts and damage to credit scores and credit reports, but also time and expense relating to:

a. Finding fraudulent charges;

b. Canceling and reissuing cards;

c. Purchasing credit monitoring and identity theft prevention;

d. Imposition of withdrawal and purchase limits on compromised accounts;

e. Inability to withdraw funds linked to compromised accounts;

f. Trips to banks and waiting in line to obtain funds held in limited accounts;

g. Resetting automatic billing instructions; and

h. Late fees and declined payment fees imposed as a result of failed automatic payments.

62. As a result, Plaintiffs and Class members now face years of constant surveillance of their financial and personal records, monitoring, and loss of rights. Plaintiffs and the Class are incurring and will continue to incur such damages in addition to any fraudulent credit and debit card charges incurred by them and the resulting loss of use of their credit and access to funds, whether or not such charges are ultimately reimbursed by the credit card companies.

Plaintiffs and Class Members Suffered Damages

63. The Data Breach was a direct and proximate result of Home Depot's failure to properly safeguard and protect Plaintiffs' and Class members' Personal Information from unauthorized access, use, and disclosure, as required by various state and federal regulations, industry practices, and the common law, including Home Depot's failure to establish and implement appropriate administrative, technical, and physical safeguards to ensure the security and confidentiality of Plaintiffs' and Class members' Personal Information to protect against reasonably foreseeable threats to the security or integrity of such information.

64. Plaintiffs' and Class members' Personal Information is private and sensitive in nature and was left inadequately protected by Home Depot. Home Depot did not obtain Plaintiffs' and Class members' consent to disclose their Personal Information to any other person as required by applicable law and industry standards.

65. As a direct and proximate result of Home Depot's wrongful actions and inaction and the resulting Data Breach, Plaintiffs and Class members have been placed at an imminent, immediate, and continuing increased risk of harm from identity theft and identity fraud, requiring them to take the time and effort to mitigate the actual and potential impact of the Data Breach on their lives including

by placing "freezes" and "alerts" with credit reporting agencies, contacting their financial institutions, closing or modifying financial accounts, and closely reviewing and monitoring their credit reports and accounts for unauthorized activity.

66. Home Depot's wrongful actions and inaction directly and proximately caused the theft and dissemination into the public domain of Plaintiffs' and Class members' Personal Information, causing them to suffer, and continue to suffer, economic damages and other actual harm for which they are entitled to compensation, including:

a. theft of their personal and financial information;

b. the imminent and certainly impending injury flowing from potential fraud and identify theft posed by their credit/debit card and personal information being placed in the hands of criminals and already misused via the sale of Plaintiffs' and Class members' information on the Internet card black market;

c. the untimely and inadequate notification of the Data Breach;

d. the improper disclosure of their Personal Information;

e. loss of privacy;

f. ascertainable losses in the form of out-of-pocket expenses and the value of their time reasonably incurred to remedy or mitigate the effects of the Data Breach;

g. ascertainable losses in the form of deprivation of the value of their PII and PCD, for which there is a well-established national and international market;

h. overpayments to Home Depot for products purchased during the Data Breach in that a portion of the price paid for such products by Plaintiffs and Class members to Home Depot was for the costs of reasonable and adequate safeguards and security measures that would protect customers' Personal Information, which Home Depot did not implement and, as a result, Plaintiffs and Class members did not receive what they paid for and were overcharged by Home Depot; and

i. the loss of use of and access to their account funds and costs associated with inability to obtain money from their accounts or being limited in the amount of money they were permitted to obtain from their accounts.

67. Plaintiffs and members of the Class also purchased products or services they otherwise would not have purchased, or paid more for those products and services than they otherwise would have paid.

CLASS ACTION ALLEGATIONS

68. Plaintiffs seek relief in their individual capacity and as representatives of all others who are similarly situated. Pursuant to Fed. R. Civ. P. 23(a) and (b)(2) and/or (b)(3), Plaintiffs seek certification of a nationwide class and a class of Florida residents. The nationwide class is defined as follows:

> All residents of the United States whose personal and/or financial information was disclosed in the data breach affecting Home Depot in 2014 (the "Class").

69. The Florida Sub-Class is defined as follows:

> All residents of Florida whose personal and/or financial information was disclosed in the data breach affecting Home Depot in 2014 (the "Florida Sub- Class").

70. Excluded from each of the above Classes are Home Depot, including any entity in which Home Depot has a controlling interest, is a parent or subsidiary, or which is controlled by Home Depot, as well as the officers, directors, affiliates, legal representatives, heirs, predecessors, successors, and assigns of Home Depot. Also excluded are the judges and court personnel in this case and any members of their immediate families.

71. **Numerosity**. Fed. R. Civ. P. 23(a)(1). The members of the Class are so numerous that the joinder of all members is impractical. While the exact number of Class members is unknown to Plaintiffs at this time, based on information and belief, it is in the millions.

72. **Commonality**. Fed. R. Civ. P. 23(a)(2) and (b)(3). There are questions of law and fact common to the Class, which predominate over any questions affecting only individual Class members. These common questions of law and fact include, without limitation:

a. Whether Home Depot engaged in the wrongful conduct alleged herein including whether Home Depot willfully, recklessly, and/or negligently failed to maintain and/or execute reasonable procedures designed to prevent unauthorized access to Plaintiffs' and Class members' Personal Information;

b. Whether Home Depot owed a duty to Plaintiffs and members of the Class to adequately protect their personal and financial information and to provide timely and accurate notice of the Data Breach to Plaintiffs and members of the Class;

c. Whether Home Depot breached its duties to protect the personal and financial information of Plaintiffs and members of the Class by

failing to provide adequate data security and whether Home Depot breached its duty to provide timely and accurate notice to Plaintiffs and members of the Class;

d. Whether Home Depot knew or should have known that its computer systems were vulnerable to attack;

e. Whether Home Depot's conduct, including its failure to act, resulted in or was the proximate cause of the breach of its systems, resulting in the loss of millions of consumers' personal and financial data;

f. Whether Plaintiffs and members of the Class suffered injury, including ascertainable losses, as a result of Home Depot's conduct or failure to act;

g. Whether Home Depot's Personal Information storage and protection protocols were reasonable under industry standards;

h. Whether Home Depot has an implied contractual obligation to use reasonable security measures;

i. Whether Home Depot breached an implied contractual obligation to use reasonable security measures;

j. Whether Home Depot violated the Florida Deceptive and Unfair Trade Practices Act, Fla. Stat. §§ 501.201, *et seq.*;

k. Whether Plaintiffs and members and Class are entitled to recover actual damages and/or statutory damages;

l. Whether Plaintiffs and Class members are entitled to equitable relief, including injunctive relief, restitution, disgorgement and/or other equitable relief.

73. All members of the purposed Classes are readily ascertainable by objective criteria. Home Depot has access to addresses and other contact information for millions of members of the Classes, which can be used for providing notice to many Class members.

74. **Typicality**. Fed. R. Civ. P. 23(a)(3). Plaintiffs' claims are typical of those of other Class members because Plaintiffs' information, like that of other class members, was misused and/or disclosed by Home Depot.

75. **Adequacy of Representation**. Fed. R. Civ. P. 23(a)(4). Plaintiffs will fairly and adequately represent and protect the interests of the members of the Class. Plaintiffs' Counsel are competent and experienced in litigating class actions.

76. **Superiority of Class Action**. Fed. R. Civ. P. 23(b)(3). A class action is superior to other available methods for the fair and efficient adjudication of this

controversy since joinder of all the members of the Class is impracticable. Furthermore, the adjudication of this controversy through a class action will avoid the possibility of inconsistent and potentially conflicting adjudication of the asserted claims. There will be no difficulty in the management of this action as a class action.

77. Damages for any individual class member are likely insufficient to justify the cost of individual litigation, so that in the absence of class treatment, Home Depot's violations of law inflicting substantial damages in the aggregate would go un-remedied without certification of the Class.

78. Class certification is also appropriate under Fed. R. Civ. P. 23(a) and (b)(2), because Home Depot has acted or has refused to act on grounds generally applicable to the Class, so that final injunctive relief or corresponding declaratory relief is appropriate as to the Class as a whole.

COUNT I

NEGLIGENCE

(On Behalf of Plaintiffs and the Class under Georgia Law)

79. Plaintiffs incorporate by reference all preceding paragraphs as if fully set forth herein.

80. To establish negligence under Georgia law, a plaintiff must plead and prove: (1) a legal duty to conform to a standard of conduct raised by the law for the

protection of others against unreasonable risks of harm; (2) a breach of this standard; (3) a legally attributable causal connection between the conduct and the resulting injury; and (4) some loss or damage flowing to the plaintiff's legally protected interest as a result of the alleged breach of the legal duty. A legal duty can arise out of the general duty one owes to all the world not to subject them to an unreasonable risk of harm.

81. Under the law of its home state, Home Depot owed a duty to Plaintiffs and members of the Class to exercise reasonable care in obtaining, retaining, securing, safeguarding, deleting and protecting their personal and financial information in its possession from being compromised, lost, stolen, accessed and misused by unauthorized persons and thus subjecting Plaintiffs and members of the Class to an unreasonable risk of harm. This duty included, among other things, designing, maintaining, and testing Home Depot's security systems to ensure that Plaintiffs' and Class members' personal and financial information in Home Depot's possession was adequately secured and protected. Home Depot further owed a duty to Plaintiffs and Class members to implement processes that would detect a breach of its security system in a timely manner and to timely act upon warnings and alerts, including those generated by its own security systems.

82. Home Depot owed a duty to Plaintiffs and members of the Class to provide security, including consistent with industry standards and requirements, to ensure that its computer systems and networks, and the personnel responsible for them, adequately protected the personal and financial information of Plaintiffs and members of the Class who used credit and debit cards to make purchases at Home Depot stores and to prevent Plaintiffs and members of the Class from being subject to an unreasonable risk of harm.

83. Home Depot owed a duty of care to Plaintiffs and Class members because they were foreseeable and probable victims of any inadequate security practices. Home Depot solicited, gathered, and stored the personal and financial data provided by Plaintiffs and members of the Class to facilitate sales transactions with its customers. Home Depot knew it inadequately safeguarded such information on its computer systems and that hackers routinely attempted to access this valuable data without authorization. Home Depot knew that a breach of its systems would cause damages to Plaintiffs and members of the Class and subject them to an unreasonable risk of harm and Home Depot had a duty to adequately protect such sensitive financial and personal information.

84. Home Depot owed a duty to timely and accurately disclose to Plaintiffs and members of the Class that their personal and financial information

had been or was reasonably believed to have been compromised. Timely disclosure was required, appropriate and necessary so that, among other things, Plaintiffs and members of the Class could take appropriate measures to avoid unauthorized charges to their credit or debit card accounts, cancel or change usernames and passwords on compromised accounts, monitor their account information and credit reports for fraudulent activity, contact their banks or other financial institutions that issue their credit or debit cards, obtain credit monitoring services and take other steps to mitigate or ameliorate the damages caused by Home Depot's misconduct.

85. Plaintiffs and members of the Class entrusted Home Depot with their personal and financial information, including when using their credit or debit cards to make purchases at Home Depot stores, on the premise and with the understanding that Home Depot would safeguard their information, and Home Depot was in a position to protect against the harm suffered by Plaintiffs and members of the Class as a result of the Data Breach.

86. Home Depot knew, or should have known, of the risks inherent in collecting and storing the personal and financial information of Plaintiffs and members of the Class who used credit and debit cards to make purchases at Home

Depot stores, and of the critical importance of providing adequate security of that information to protect its customers from the unreasonable risk of harm.

87. Home Depot's own conduct also created a foreseeable risk of harm to Plaintiffs and members of the Class. Home Depot's misconduct included, but was not limited to, its failure to take the steps and opportunities to prevent and stop the Data Breach as set forth herein. Home Depot's misconduct also included its decision not to comply with industry standards for the safekeeping and maintenance of the personal and financial information of Plaintiffs and Class members.

88. Home Depot breached the duties it owed to Plaintiffs and members of the Class by failing to exercise reasonable care and implement adequate security systems, protocols and practices sufficient to protect the personal and financial information of Plaintiffs and members of the Class.

89. Home Depot breached the duties it owed to Plaintiffs and Class members by failing to properly implement technical systems or security practices that could have prevented the loss of the data at issue.

90. Home Depot breached its duties to timely and accurately disclose that Plaintiffs' and Class members' personal and financial information in Home

Depot's possession had been or was reasonably believed to have been, stolen or compromised.

91. Home Depot's failure to comply with its legal obligations and with industry standards and regulations, such as PCI DSS, and the delay between the date of intrusion and the date Home Depot disclosed the data breach further evidence Home Depot's negligence in failing to exercise reasonable care in safeguarding and protecting Plaintiffs' and Class members' personal and financial information in Home Depot's possession.

92. But for Home Depot's wrongful and negligent breach of its duties owed to Plaintiffs and members of the Class, their personal and financial information would not have been compromised.

93. The injury and harm suffered by Plaintiffs and members of the Class as set forth above was the reasonably foreseeable result of Home Depot's failure to exercise reasonable care in safeguarding and protecting Plaintiffs' and Class members' personal and financial information within Home Depot's possession. Home Depot knew or should have known that its systems and technologies for processing, securing, safeguarding and deleting Plaintiffs' and Class members' personal and financial information were inadequate and vulnerable to being breached by hackers.

94. Plaintiffs and members of the Class suffered injuries and losses described herein as a direct and proximate result of Home Depot's conduct resulting in the data breach, including Home Depot's lack of adequate reasonable and industry-standard security measures. Had Home Depot implemented such adequate and reasonable security measures, Plaintiffs and Class members would not have suffered the injuries alleged, as the Home Depot data breach would likely have not occurred.

95. A special relationship exists between Plaintiffs and members of the Class and Home Depot. Home Depot invited Plaintiffs and members of the Class, as customers, to use their credit or debit cards in making purchases at Home Depot stores, including during the period of the Home Depot data breach, with the mutual understanding that Home Depot had reasonable security measures in place to protect its customers' personal and financial information.

96. Home Depot's conduct warrants moral blame, as Home Depot continued to take possession of Plaintiffs' and Class members' personal and financial information in connection with Home Depot sales knowing, and without disclosing, that it had inadequate systems to reasonably protect such information, that the data breach had occurred and was ongoing for nearly five months, and

Home Depot failed to provide timely and adequate notice to Plaintiffs and members of the Class of the Data Breach.

97. As a direct and proximate result of Home Depot's negligent conduct, Plaintiffs and the Class have suffered injury and are entitled to damages in an amount to be proven at trial.

COUNT II

BREACH OF IMPLIED CONTRACT
(On Behalf of Plaintiffs and the Class under Georgia Law)

98. Plaintiffs incorporate by reference all preceding paragraphs as if fully set forth herein.

99. Home Depot solicited and invited Plaintiffs and Class members to purchase products at Home Depot's stores using their credit or debit cards. Plaintiffs and Class members accepted Home Depot's offers and used their credit or debit cards to purchase products at Home Depot's stores during the period of the Data Breach.

100. When Plaintiffs and Class members provided their Personal Information to Home Depot to make purchases at Home Depot's stores, including but not limited to the Personal Information contained on the face of, and embedded in the magnetic strip of, their debit and credit cards, Plaintiffs and Class members entered into implied contracts with Home Depot pursuant to which Home Depot

agreed to safeguard and protect such information and to timely and accurately notify Plaintiffs and Class members if their data had been breached and compromised.

101. Each purchase at a Home Depot store made by Plaintiffs and Class members using their credit or debit card was made pursuant to the mutually agreed-upon implied contract with Home Depot under which Home Depot agreed to safeguard and protect Plaintiffs' and Class members' Personal Information, including all information contained in the magnetic stripe of Plaintiffs' and Class members' credit or debit cards, and to timely and accurately notify them if such information was compromised or stolen.

102. Plaintiffs and Class members would not have provided and entrusted their Personal Information, including all information contained in the magnetic stripes of their credit and debit cards, to Home Depot to purchase products at Home Depot's stores in the absence of the implied contract between them and Home Depot.

103. Plaintiffs and Class members fully performed their obligations under the implied contracts with Home Depot.

104. Home Depot breached the implied contracts it made with Plaintiffs and Class members by failing to safeguard and protect the Personal Information of

Plaintiffs and Class members and by failing to provide timely and accurate notice to them that their Personal Information was compromised in and as a result of the Data Breach.

105. As a direct and proximate result of Home Depot's breaches of the implied contracts between Home Depot and Plaintiffs and Class members, Plaintiffs and Class members sustained actual losses and damages as described in detail in this Complaint.

COUNT III

VIOLATION OF THE FLORIDA DECEPTIVE AND UNFAIR TRADE PRACTICES ACT (Fla. Stat. §§ 501.201, *et seq*.)

(On Behalf of Plaintiff Gilchrist and the Florida Sub-Class)

106. Plaintiffs incorporate by reference all preceding paragraphs as if fully set forth herein.

107. The Florida Deceptive and Unfair Trade Practices Act (Fla. Stat. §§ 501.201, *et seq*.) ("FDUTPA") declares that "unfair or deceptive acts or practices in the conduct of any trade or commerce" are unlawful. Fla. Stat. § 501.204(1). Under the FDUTPA, any person who has suffered losses as a result of a violation may commence a private action to recover actual damages, attorney's fees, and costs. Fla. Stat. § 501.211(2).

108. At all relevant times, Home Depot provided goods and/or services and thereby was engaged in trade or commerce.

109. Home Depot engaged in deceptive representations and/or omissions and unfair acts and practices by knowingly using out-of-date security software and failing to implement adequate security systems, protocols and practices sufficient to protect the personal and financial information of Plaintiff Gilchrist and the Florida Sub-Class.

110. Had Plaintiff Gilchrist and the Florida Sub-Class known of Home Depot's failure to maintain adequate security measures to protect their Private Information, Plaintiff Gilchrist and the Florida Sub-Class would not have made purchases at Home Depot stores or otherwise entrusted their Personal Information to Home Depot.

111. Home Depot further deceived and engaged in unfair practices towards Plaintiff Gilchrist and the Florida Sub-Class by failing to timely notify and disclose to its customers the existence and scope of the Data Breach.

112. Plaintiff and Class Members have a vested interest in the privacy, security and integrity of their Personal Information, therefore, this interest is a "thing of value" as contemplated by FDUTPA.

113. Home Depot's practices and course of conduct, as alleged herein, is likely to mislead—and has misled—Florida consumers acting reasonably in the circumstances, to the consumers' detriment.

114. Home Depot has engaged in an unfair practice that offends established public policy, and is one that is immoral, unethical, oppressive, unscrupulous and/or substantially injurious to Florida consumers.

115. Plaintiff Gilchrist and the Florida Sub-Class have suffered actual injury as a direct result of Home Depot's deceptive representations and/or omissions and unfair acts and practices, including: (a) fraudulent charges on their credit and debit accounts; (b) damage to credit scores and credit reports; and (c) time and expense related to: (i) finding fraudulent charges; (ii) canceling and reissuing cards; (iii) purchasing credit monitoring and identity theft prevention; (iv) imposition of withdrawal and purchase limits on compromised accounts; (v) inability to withdraw funds linked to compromised accounts; (vi) trips to banks and waiting in line to obtain funds held in limited accounts; (vii) resetting automatic billing instructions; (viii) late fees and declined payment fees imposed as a result of failed automatic payments; and (ix) the anxiety, distress, nuisance and annoyance of experiencing present and potential future harm as a result of the Data Breach.

116. Plaintiff Gilchrist and the Florida Sub-Class are entitled to preliminary and permanent injunctive relief without proof of monetary damage, loss of profits, or intent to deceive. Plaintiff Gilchrist and the Florida Sub-Class seek equitable relief and to enjoin Defendant on terms that the Court considers appropriate.

117. At all relevant times, Home Depot's deceptive trade practices are willful within the meaning of FDUTPA and, accordingly, Plaintiff Gilchrist and the Florida Sub-Class are entitled to an award of attorneys' fees, costs and other recoverable expenses of litigation.

REQUEST FOR RELIEF

WHEREFORE, Plaintiffs, on behalf of themselves and the Classes set forth herein, respectfully request the following relief:

a. That the Court certify this case as a class action pursuant to Fed. R. Civ. P. 23(a), (b)(2) and/or (b)(3), and, pursuant to Fed. R. Civ. P. 23(g), appoint the named Plaintiffs to be Class representatives and their undersigned counsel to be Class counsel;

b. That the Court award Plaintiffs and the Classes appropriate relief, including actual and statutory damages, restitution and disgorgement;

c. That the Court award Plaintiffs and the Class equitable, injunctive and declaratory relief as maybe appropriate under applicable state laws. Plaintiffs, on behalf of the Classes, seek appropriate injunctive relief designed to ensure against the recurrence of a data breach by adopting and implementing best security data practices to safeguard customers' financial and personal information and that would include, without limitation, an order and judgment directing Home to (1) encrypt all sensitive cardholder data beginning within the device to which the cards are presented for purchase (*e.g.*, PIN pad) and continuing until the data reaches Home Depot's payment processor or payment switch; (2) comply with the Payment Card Data Security Standard (PCI DDS); (3) directing Home Depot to provide to Plaintiffs and Class members extended credit monitoring services; (4) equitable relief requiring restitution and disgorgement of the revenues wrongfully retained as a result of Home Depots' wrongful conduct; and (5) relief enjoining Home Depot from engaging in the wrongful conduct complained of herein pertaining to the misuse and/or disclosure of Plaintiffs and Class members' private information, and from

refusing to issue prompt, complete and accurate disclosures to the Plaintiffs and Class members;

d. That the Court award Plaintiffs and the Classes actual damages, compensatory damages, statutory damages, and statutory penalties, to the full extent permitted by law, in an amount to be determined;

e. That the Court award Plaintiffs and the Classes pre-judgment and post-judgment interest;

f. That the Court award Plaintiffs and the Classes reasonable attorney fees and costs as allowable by law; and

g. That the Court award Plaintiffs and the Classes such other, favorable relief as allowable under law or at equity.

DEMAND FOR JURY TRIAL

Plaintiffs demand a jury trial of all claims to the extent authorized by law.

Dated: September 24, 2014

THE BARNES LAW GROUP, LLC

By: /s/ROY E. BARNES

Roy E. Barnes (Ga. Bar No. 039000)
John R. Bevis (Ga. Bar No. 056110)
31 Atlanta Street
Marietta, Georgia 30060
Tel.: 770-419-8505; Fax: 770-590-8958
roy@barneslawgroup.com
bevis@barneslawgroup.com

STUEVE SIEGEL HANSON LLP
Norman E. Siegel (*pro hac vice forthcoming*)
Barrett J. Vahle (*pro hac vice forthcoming*)
John Austin Moore (*pro hac vice forthcoming*)
460 Nichols Road, Suite 200
Kansas City, Missouri 64112
Tel.: 816-714-7100
Fax: 816-714-7101
siegel@stuevesiegel.com
vahle@stuevesiegel.com
moore@stuevesiegel.com

STUEVE SIEGEL HANSON LLP
Darren T. Kaplan (Georgia Bar No. 172670)
1359 Broadway
Suite 2001
New York, NY 10018
Tel: (212) 999-7370
Fax: (816) 714-7101
kaplan@stuevesiegel.com

ATTORNEYS FOR PLAINTIFFS